IN THE DRAWING

The Examiner objected to Figs. 1-4, 20 and 28-30 as requiring the label "Prior Art". Accordingly, Applicants submit herewith a Transmittal of Corrected Formal Drawings, with Figs. 1-4, 20 and 28-30 labeled "Prior Art" as replacement sheets.

A replacement sheet showing corrected Fig. 16B is also included, changing "BP" to BQ.

REMARKS

The Applicants request reconsideration of the rejection.

Claims 5-13 were examined, Claims 1-4 having been withdrawn pursuant to a Restriction Requirement.

The Examiner requires a "prior art" legend to be added to Figures 1-4, 20, and 28-30. Replacement sheets for these figures, containing the required legend, accompany this Reply.

The Examiner also objected to the drawings as containing reference characters not mentioned in the description. The specification has been amended above to add reference numbers corresponding to those noted by the Examiner.

The Examiner also objected to the drawings as containing minor informalities. Replacement sheets for the indicated drawings are also included to address the Examiner's concerns.

The Examiner also objected to the disclosure as containing minor informalities as noted on Pages 4-5 of the Office Action. The specification has been amended to address the Examiner's concerns.

The claims were found objectionable as containing undesirable numerals in parentheses. The amendments to the claims address this matter as well.

Claims 5-10 were rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al., U.S. 6,278,783 (Kocher).

The Applicants respectfully traverse, noting that Kocher discloses a technique for improving DES and other cryptographic protocols against external monitoring attacks by reducing the amount of useful information leaked during processing. More specifically, Kocher prepares two 56-bit keys (KY1 and KY2) corresponding to a secret key K. K1 is an arbitrary random number and K2 is derived by K2 = K XOR KY1. Then, Kocher makes a random permutation K1P of KY and a random permutation K2P of K2. KY1P and KY2P are created such that KYP{KY1} XOR K2P{K2} equals the standard DES key K.

A fundamental difference between Kocher's technique for improving DES and other cryptographic protocols and the present invention is that Kocher changes the bit sequences of the keys K1 and K2, whereas the present invention does not change the bit sequences of data A and data B because the data are loaded in accordance with each bit sequence. That is, the present invention changes the order of register loading of the data bits, but Kocher loads keys K1 and K2 into registers R1 and R2, respectively, and then performs an XOR operation on

the contents of these two registers. Further, when loading the keys into the registers, Kocher permutes the sequence of K1 by K1P and of K2 of K2P, such that the following series of operations must be performed: R1 load, R2 load, arithmetic operation, R1 load, R2 load, arithmetic operation, R1 load, R2 load, arithmetic operation, ...

Thus, in randomly changing the order of register loading, without changing the bit sequences of data A and data B, the present invention is patentably distinguishable from Kocher. In the language of Claim 5, Kocher does not perform steps of selecting either: after transferring one operation unit in the bit pattern of data A in a memory in order of its bit sequence to a first register R1, transferring one operation unit in the bit pattern of data B in the memory in order of its bit sequence to a second register R2; or after transferring one operation unit in the bit pattern of said data B in order of its bit sequence to the second register R2, transferring one operation in the bit pattern in said data A in order of its bit sequence to the first register R1. Further, Kocher does not execute a predetermined arithmetic operation on the contents of the first register R1 and the contents of the

second register R2, store the result of the arithmetic operation, and repeat the method steps until the arithmetic operation for data A and data B is finished.

Regarding independent Claim 6, Kocher does not perform the steps of selecting either transferring one operation unit of data A in a memory in order of its bit sequence to a first register R1, and transferring one operation unit of data B in order of its bit sequence to a second register R2; or transferring the one operation unit of data A in order of its bit sequence to the second register R2 and transferring the one operation unit of data B in order of its bit sequence to the first register R1. Further, Kocher does not execute a predetermined arithmetic operation on the contents of the first register R1 and the contents of the second register R2, store the result of the arithmetic operation in the memory, and repeat the method steps until the arithmetic operation on data A and data B is finished.

Claims 11-13 were rejected under 35 U.S.C. 102(e) as being anticipated by Jahnich et al., U.S. 6725,374 (Jahnich). The Applicants traverse as follows.

Claim 11 includes steps of selecting any of an unprocessed operation unit in a bit pattern of data A in a memory, transferring the selected operation unit to a first register R1, and transferring one operation unit in a bit pattern of data B in the memory corresponding to the operation unit selected from data A to a second register R2.

Jahnich, on the other hand, discloses the order of execution of an encryption program executed on a microprocessor-mounted card, but randomly permutes the serial order of execution of subprograms in the execution of the encryption program. Thus, while Jahnich teaches a technique of randomly replacing the start address of a subprogram with the start address of another subprogram, Jahnich fails to suggest the data processed by either subprogram. Necessarily, therefore, Jahnich neither discloses nor suggests how each subprogram might process an operation unit of data A or data B as claimed. Further, Jahnich does not disclose or fairly suggest how to select randomly an operation unit from among the bit sequences of data A or B.

Thus, even considering Jahnich as disclosed, the person of ordinary skill would never learn to draw a correspondence

between a subprogram and an operation unit of data, which would be required for that person of ordinary skill to derive the presently claimed invention from the disclosure of Jahnich.

In view of the foregoing amendments and remarks, the Applicants respectfully request reconsideration of the rejection and allowance of the claims.

Respectfully submitted,

Daniel J. Stanger
Registration No. 32,846
Attorney for Applicants

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Road, Suite 370
Alexandria, Virginia 22301
(703) 684-1120
Date: February 3, 2006